



PROPOSED RULE MAKING

CR-102 (June 2012)

(Implements RCW 34.05.320)

Do **NOT** use for expedited rule making

Agency: Office of Insurance Commissioner

- ☒ **Preproposal Statement of Inquiry** was filed as WSR 12-10-081; or
☐ **Expedited Rule Making--Proposed notice** was filed as WSR _____; or
☐ **Proposal is exempt under RCW 34.05.310(4) or 34.05.330(1).**

- ☒ **Original Notice**
☐ **Supplemental Notice to WSR**

☐ **Continuance of WSR** _____

Title of rule and other identifying information: Security Breach Notification

Insurance Commissioner Matter No. R 2012-14

Hearing location(s):

Insurance Commissioner's Office
 TR 120
 5000 Capitol Blvd.
 Tumwater, WA 98504-0255

Date: December 27, 2012 Time: 10:00am

Submit written comments to:

Name: Donna Dorris
 Address: PO Box 40258, Olympia WA 98504-0258
 e-mail rulescoordinator@oic.wa.gov
 fax (360) 586-3109 by December 27, 2012

Assistance for persons with disabilities: Contact

Lorie Villaflores by December 26, 2012

TTY (360) 586-0241 or (360) 725-7087

Date of intended adoption: January 2, 2013
 (Note: This is **NOT** the **effective** date)

Purpose of the proposal and its anticipated effects, including any changes in existing rules: The proposed rule will identify who is required to be notified when a security breach occurs and what information is required to be included in the notification. The proposed regulation will provide consistency between state and federal requirements.

Reasons supporting proposal: In 2009, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) was amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act. The changes affect notice requirements related to security breaches, such as unintentional disclose of personal health information. State regulations will be consistent with federal requirements.

Statutory authority for adoption: RCW 48.02.060, 48.30.010 & 48.43.505. The Gramm-Leach Bliley Act, Pub. L. 102-106, Sec. 501(b), Sec. 505(B)(2). The Health Information Technology for Economic and Clinical Health Act, Pub. L. 111-5, Sec.13402.

Statute being implemented: RCW 48.43.505.

Is rule necessary because of a:

- Federal Law? ☐ Yes ☐ No
 Federal Court Decision? ☐ Yes ☐ No
 State Court Decision? ☒ Yes ☐ No
 If yes, CITATION:
 The Gramm-Leach Bliley Act, Pub. L. 102-106, Sec. 501(b), Sec. 505(B)(2). The Health Information Technology for Economic and Clinical Health Act, Pub. L. 111-5, Sec.13402.

DATE
 November 20, 2012

NAME (type or print)
 Mike Kreidler

SIGNATURE

Mike Kreidler

TITLE
 Insurance Commissioner

CODE REVISER USE ONLY

OFFICE OF THE CODE REVISER
 STATE OF WASHINGTON
 FILED

DATE: November 20, 2012

TIME: 8:36 AM

WSR 12-23-071

(COMPLETE REVERSE SIDE)

Agency comments or recommendations, if any, as to statutory language, implementation, enforcement, and fiscal matters: None

Name of proponent: Mike Kreidler, Insurance Commissioner

☐ Private
☐ Public
☒ Governmental

Name of agency personnel responsible for:

Name	Office Location	Phone
Drafting..... Donna Dorris	PO Box 40258, Olympia, WA 98504-0258	(360) 725-7040
Implementation....John Hamje	PO Box 40255, Olympia, WA 90504-0255	(360) 725-7262
Enforcement.....Carol Sureau	PO Box 40255, Olympia, WA 98504-0255	(360) 725-7050

Has a small business economic impact statement been prepared under chapter 19.85 RCW or has a school district fiscal impact statement been prepared under section 1, chapter 210, Laws of 2012?

☐ Yes. Attach copy of small business economic impact statement or school district fiscal impact statement.

A copy of the statement may be obtained by contacting:

Name:

Address:

phone () _____

fax () _____

e-mail _____

☒ No. Explain why no statement was prepared.

The increased cost for insurance licensees to meet this proposed new requirement (notifying the commissioner in cases of a security breach) is significantly less than 0.3% of the average Washington revenue of the smallest domestic licensees. Therefore an SBEIS is not required for this proposed rule.

Is a cost-benefit analysis required under RCW 34.05.328?

☒ Yes A preliminary cost-benefit analysis may be obtained by contacting:

Name: Donna Dorris

Address: PO Box 40258

Olympia, WA 98504-0258

phone (360) 725-7040

fax (360) 586-3109

e-mail rulescoordinator@oic.wa.gov

☐ No: Please explain:

AMENDATORY SECTION (Amending Matter No. R 2000-08, filed 1/9/01, effective 2/9/01)

WAC 284-04-610 Violation. A violation of this (~~regulation~~) chapter shall be deemed to be an unfair method of competition or an unfair or deceptive act and practice in this state.

NEW SECTION

WAC 284-04-625 Security breach notification requirements.

(1) The commissioner defines failure to provide notice of security breaches in compliance with this section as an unfair practice for the following reasons:

(a) Many licensees fail or periodically fail to protect personal information and protected health information as defined in subsection (2)(a) and (b) of this section, resulting in security breaches affecting their customers or consumers.

(b) When a customer or consumer whose personal or protected health information has been breached seeks assistance from the commissioner, information about security breaches and what actions a licensee is taking to protect customers or consumers must be available to the commissioner.

(2) All licensees must notify the insurance commissioner in writing within two business days about the number of customers or consumers potentially affected and what actions are being taken following discovery of:

(a) A breach of personal information as defined in RCW 19.255.010 (4) and (5) that seems reasonably likely to subject customers to a risk of criminal activity; or

(b) A breach of unsecured protected health information as defined in 45 C.F.R. 164.402 which compromises the security or privacy of the protected information for licensees subject to 45 C.F.R. 164.

(3) For breaches of protected health information, licensees subject to 45 C.F.R. 164 must comply with the regulations (45 C.F.R. 164.400 through 164.410) adopted by the U.S. Department of Health and Human Services (HHS) governing these requirements including:

(a) Notification requirements for a security breach as defined by 45 C.F.R. 164.400, meaning an acquisition, access, use, or disclosure of protected health information in a manner not permitted by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule which compromises the security or

privacy of the protected health information.

(b) Notifying individuals, and other entities described in 45 C.F.R. 164.404 through 164.410.

(c) Notifying affected entities without unreasonable delay and in no case later than sixty calendar days following the discovery of the breach.

(d) Notifying documents that contain:

(i) A brief description of what happened, including the date of the breach and the date of discovery of the breach, if known;

(ii) A description of the types of unsecured protected health information involved in the breach;

(iii) Any steps individuals should take to protect themselves from potential harm resulting from the breach;

(iv) A brief description of what the covered entity is doing to investigate the breach, to mitigate harm to individuals and to protect against any further breaches; and

(v) Contact information for individuals to ask questions or learn additional information.